Applicant's response:

(A) Since, as discussed above, the system derived from Schneier's teaching in view of Ginzboorg et al. and Walker et al. does not result in a system that is sufficiently similar to Chen's system and does not really predict the feature of Chen's system, we can discuss Thompson et al. on its own without referring back to the other three prior arts since they have been proven to be unrelated. The only part in Chen's system that is relevant to Thompson et al.'s method is the group method suggested by Chen.

(B) Other than the fact that they both sign the messages at different times, Chen's group method and Thompson et al. differs in the following significant ways. These differences make Thompson's method unusable and irrelevant to Chen's method.

(a) Thompson et al. suggested a method of monitoring subsequent changes made to an original document. This is fundamentally different from Chen's method. In Chen's method, there is no original document and each constituent part of the composite message is really independent from each other. Each member in the composite message adds his own data to the composite message to communicate directly with the service provider. This data is protected from other member's access. Chen uses the group method to allow the service provider to control the integrity and security of each transaction by allowing all participating members to perform the transaction steps together, instead of individually. Piggybacking or transmission efficiency is not one of its main concerns here.

(b) In Thompson's method, there is a "temporal" dependency built into the system – each level of change is dependent on the previous level. This temporal dependency is one of its main vulnerability as the recipient of a document at change level 2, for example, has no way of finding out the existence of higher level changes, if they exist. In Chen's method, members can join the composite message in any order and the service provider can use the final message to verify the completeness of the message for the transaction. There is no vulnerability of temporal dependency in Chen's system.

SUMMARY

(1) Chen's invention does not claim novelty on the use of smart car, or the use of public key technology, or the use of session key, etc. Rather Chen's novelty is on the fact that, using these items as building blocks, Chen's system is able to demonstrate a secure

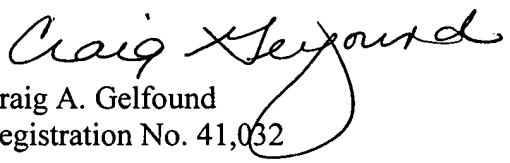
and efficient system and method that is not predicted and cannot be derived from all prior arts in the field.

(2) The office Action has not established a viable way to combine all the relevant prior art in the field to arrive at a system that bears some similarity to Chen's system. Nor has it shown that this can be done by a person with ordinary skill in the field. Allowance for patent is therefore respectfully requested.

CONCLUDING REMARKS

In view of the foregoing remarks, it is clear that the present invention is not disclosed by the combination of references cited by the Patent Office. Accordingly, Applicant respectfully submits that this application is now in condition for allowance, and reconsideration and allowance are respectfully requested.

Respectfully submitted,



Craig A. Gelfound
Registration No. 41,032

McDERMOTT, WILL & EMERY
2049 Century Park East, 34th Floor
Los Angeles, CA 90067
(310) 277-4110
Facsimile: (310) 277-4730
Date: December 23, 2003

FIG. 2

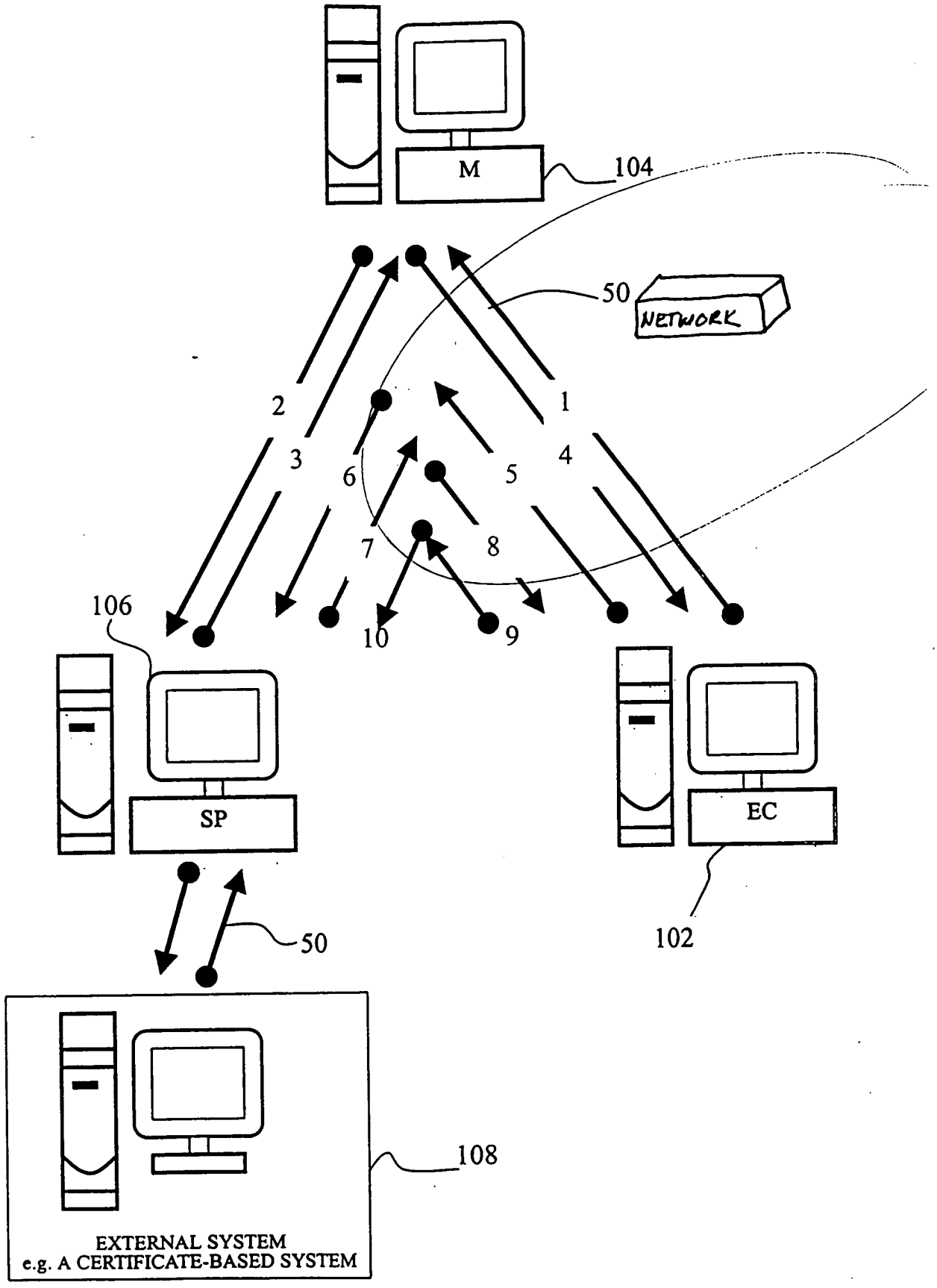
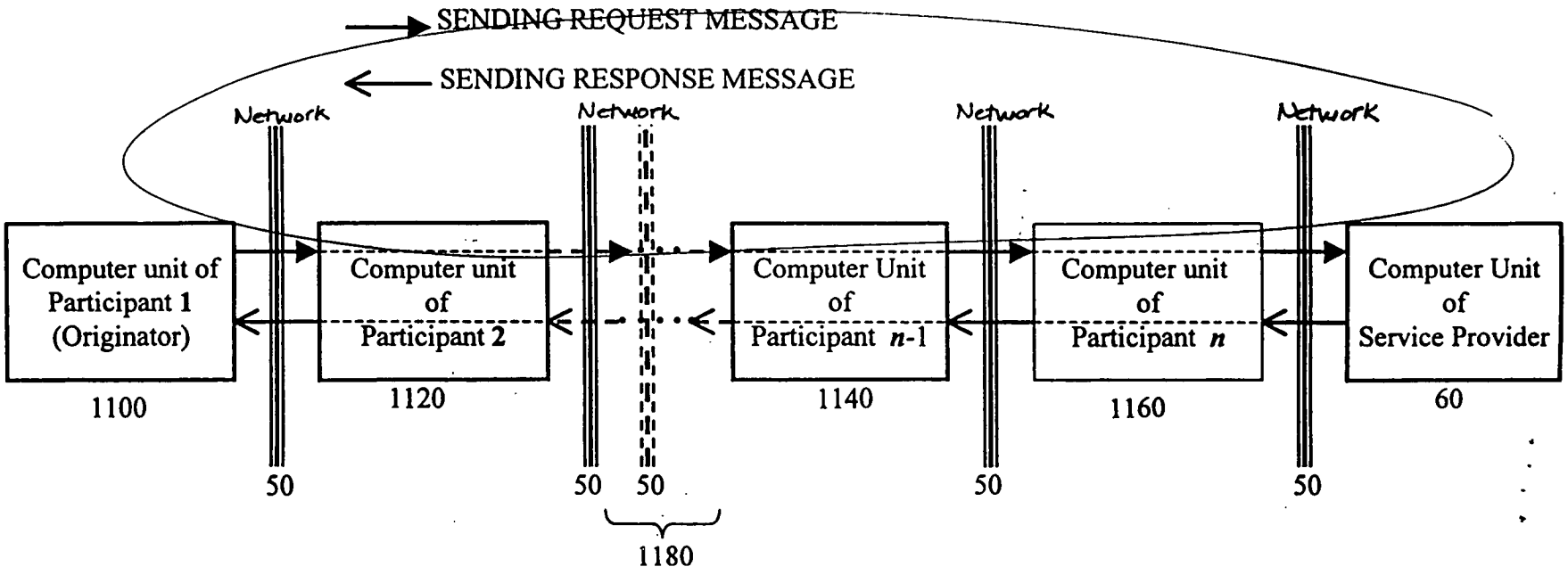

M
104
50
NETWORK
1
2
3
4
5
6
7
8
9
10
106
SP
EC
102
50
108
EXTERNAL SYSTEM
e.g. A CERTIFICATE-BASED SYSTEM

FIG. 12


SENDING REQUEST MESSAGE
SENDING RESPONSE MESSAGE
Network
Network
Network
Network
Computer unit of Participant 1 (Originator)
Computer unit of Participant 2
Computer Unit of Participant n-1
Computer unit of Participant n
Computer Unit of Service Provider
1100
1120
1140
1160
60
50
50
50
50
50
1180